Министерство образования Кировской области

«Обеспечение безопасности персональных данных»

Докладчик:

Городилов Сергей Викторович

Руководитель направления ИБ, АСПЕКТ-СЕТИ

gors@aspectspb.ru

46-56-46, 30-13-23

Важные замечания!!!

- Ответственность за реализацию конкретных правовых и организационных мер на своей территории и в рамках своей организации несет её руководитель
- Представленные материалы являются результатом опыта работы докладчика в данной сфере, основанного на доступных на данный момент времени трактовках законодательства,
- Представленные формы, материалы и презентации не являются официальной позицией государства в сфере персональных данных
- Официальную трактовку тех или иных позиций законодательства и нормативных документов в области персональных данных осуществляют: Министерство связи и массовых коммуникаций РФ, Роскомнадзор РФ (только в рамках контроля и надзора), Суды РФ, а также ФСБ, ФСТЭК, Роструд и другие органы власти в рамках своей сферы компетенции.

Дополнения к семинару №4

ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Форма заявления на компенсацию родительской платы

- Постановлением Правительства Кировской области от 26.02.2007 № 85/80 на основании полномочий, данных 273-ФЗ, установлены:
  - форма заявления;
  - необходимый перечень документов.
- Формы отдельных документов, предъявляемых на компенсацию, не могут быть изменены (Акты ГС, справки о доходах, трудовые книжки), а отдельные в них поля предоставлены в форме по желанию заявителя (национальность в свидетельстве о рождении).

Соответственно:

1. Основания для обработки принимаемых документов имеются, поскольку имеется нормативный документ.
2. Оператор не имеет целей для обработки отдельных данных (национальности), если не собирает их с использованием собственных форм учета или баз данных.

Данная логика применима:

1. При комплектовании групп в детских садах (муниципальная услуга).
2. При зачислении в общеобразовательные организации (муниципальная и государственная услуга).

Политика ПДн

Цель – сообщить субъекту ПДн, кратко, исчерпывающе и понятно:

- Цели обработки ПДн (виды деятельности)
- Субъекты ПДн (чьи данные обрабатываются)
- Основания
- Кратко о порядке обработки ПДн
- Обязательства о конфиденциальности и безопасности ПДн
- Краткие сведения о применяемых мерах, в т.ч. о хранении
- Права субъекта ПДн
- Особенности предоставления ПДн третьим лицам
- Порядок публикации и изменений
- Контактная информация

Рекомендации Роскомнадзора РФ по составлению Политики

https://rkn.gov.ru/personal-data/p908/

РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ДОКУМЕНТА, ОПРЕДЕЛЯЮЩЕГО ПОЛИТИКУ ОПЕРАТОРА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, В ПОРЯДКЕ, УСТАНОВЛЕННОМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 27 ИЮЛЯ 2006 ГОДА № 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

1. Настоящие Рекомендации разработаны в целях выработки унифицированных подходов к структуре и форме документа, определяющего политику оператора в отношении обработки персональных данных (далее – Политика).

2. Основные понятия, используемые в Рекомендациях:

– персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

– оператор персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с

ПЛАН СЕМИНАРОВ

Организационно-правовая часть

№	Дата проведения	Тема
1.	23.11.2017	Основы информационной безопасности. Персональные данные и другие категории конфиденциальной информации. Законодательство и нормативные документы в области защиты персональных данных
2.	14.12.2017	Правовые меры защиты персональных данных - КАДРЫ
3.	18.01.2018	Правовые меры защиты персональных данных – Образовательная деятельность

Организационно-техническая часть

4.	08.02.2018	Организационные меры защиты персональных данных
5.	27.02.2018	Информационные системы персональных данных (ИСПДн)
6.	15.03.2018	Модель угроз ПДн. Порядок защиты ИСПДн
7.	05.04.2018	Средства обеспечения ИБ в различных сценариях
8.	19.04.2018	Аттестация, сертификация и лицензирование в области защиты персональных данных. Контроль в области защиты персональных данных

Семинар №5

ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ФЗ-152 «О персональных данных»

Статья 1. Сфера действия настоящего Федерального закона

- отношения, связанные с обработкой персональных данных
- все организации и физические лица
- **с использованием средств автоматизации (ПК)**
- без использования средств автоматизации (ПК), если обработка персональных данных похожа на автоматизированную (по алгоритму, накопление, систематизация)

ФЗ-152 «О персональных данных»

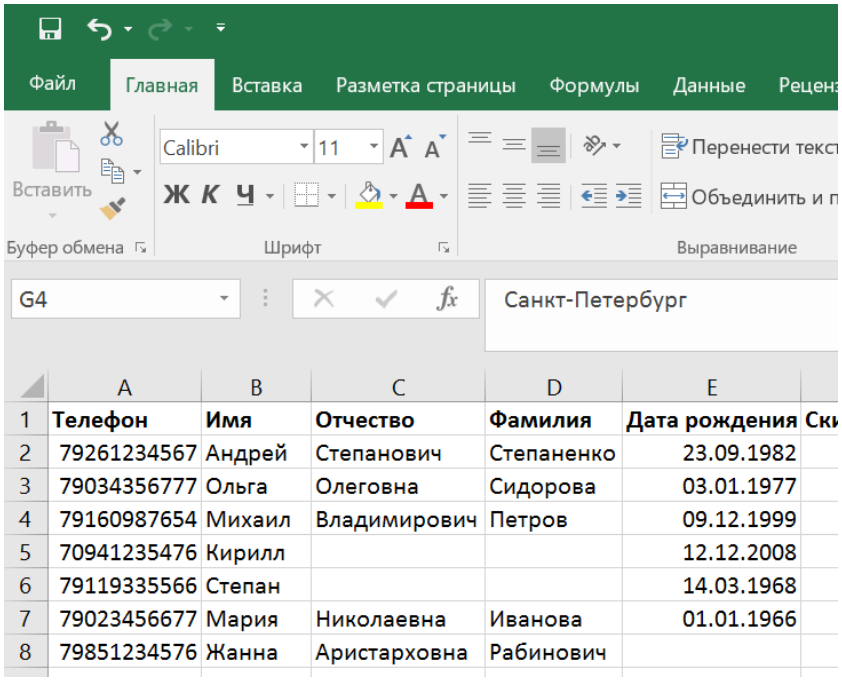
Статья 3. Основные понятия, используемые в настоящем Федеральном законе

4) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

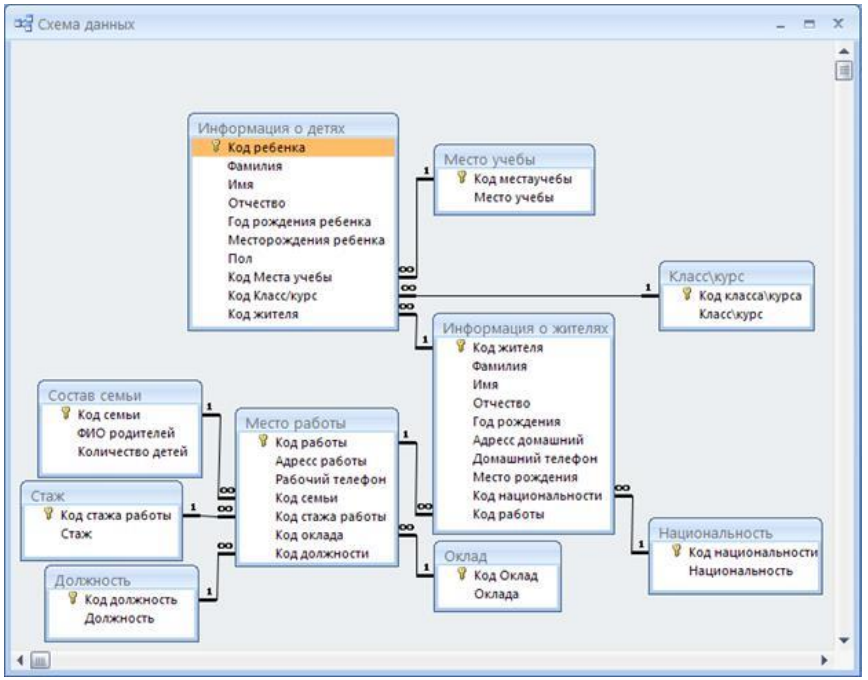
10) **информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

База данных (БД)

- Множество определений
- Более 50 видов



	A	B	C	D	E
1	**Телефон**	**Имя**	**Отчество**	**Фамилия**	**Дата рождения**
2	79261234567	Андрей	Степанович	Степаненко	23.09.1982
3	79034356777	Ольга	Олеговна	Сидорова	03.01.1977
4	79160987654	Михаил	Владимирович	Петров	09.12.1999
5	70941235476	Кирилл			12.12.2008
6	79119335566	Степан			14.03.1968
7	79023456677	Мария	Николаевна	Иванова	01.01.1966
8	79851234576	Жанна	Аристарховна	Рабинович	



База данных – ГК РФ, ст.1260

- **Базой данных** является представленная в объективной форме совокупность самостоятельных материалов (статей, расчётов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

База данных - ГОСТ Р ИСО МЭК ТО 10032-2007

- **База данных** — совокупность данных, хранимых в соответствии со схемой данных, манипулирование которыми выполняют в соответствии с правилами средств моделирования данных

К ИСПДн относятся

- ИАС АРМ «Директор»
- 1С:Бухгалтерия
- На компьютерах: Папки с документами
- Файлы Excel, Word, Access, PDF и т.п.
- Файлы XML, HTML и т.п.
- Компьютеры и терминалы, имеющие доступ к ИСПДн

Группировка и наименование?

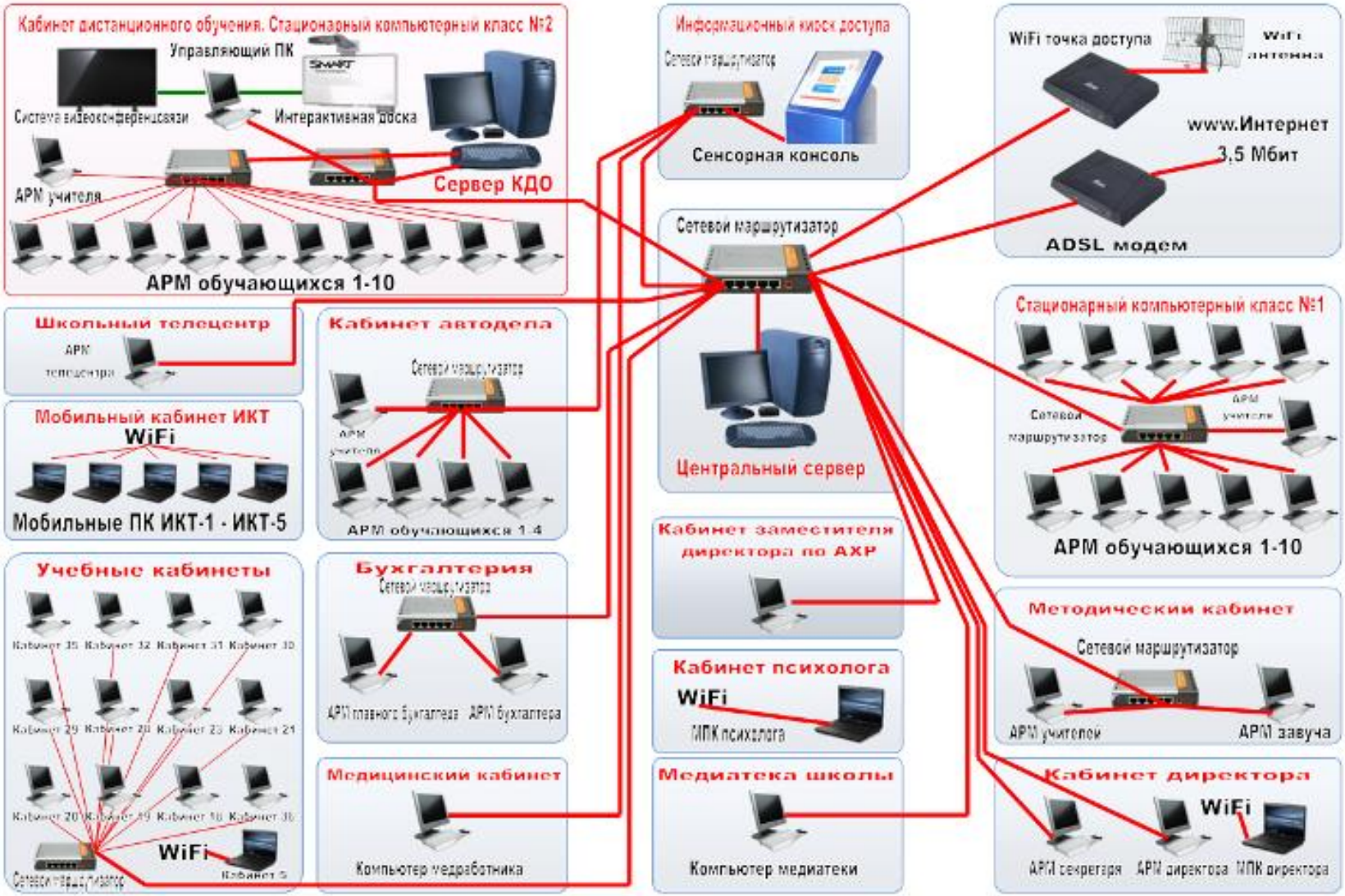
Необходимо ИСПДн определить и назвать в целях:

1. Классификации
2. Оценки угроз безопасности
3. Определения мер и выполнения защиты

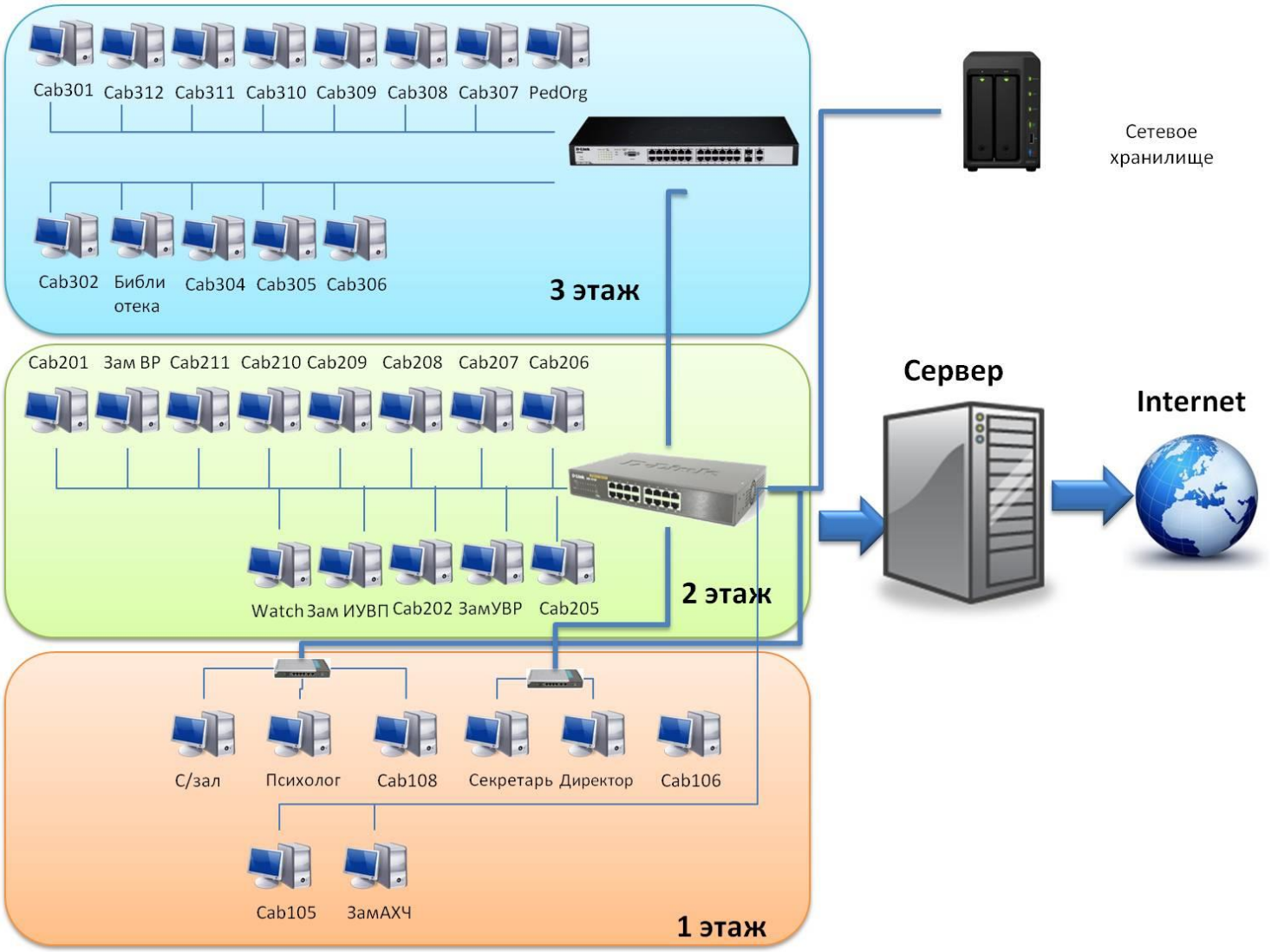
Но есть проблемы:

1. Базы данных могут находиться на всех компьютерах и серверах организации.
2. Доступ к ним могут иметь многие компьютеры и пользователи.

Пример школьной сети



Или такая сеть ОО



Группировка и наименование

ИСПДн определяют (выделяют):

1. Разделяют по назначению, например:
    1. Кадры и бухгалтерия
    2. Образовательная деятельность
2. По ресурсу, содержащему наибольшее число записей - БД, ИС

Перечень внутренних ИСПДн

№ п/п	Наименование ИСПДн	Архитектура	Кол-во мест	Категория ПДн	Объем ПДн	ПДн Сотрудников / 3-х лиц	Тип актуальных угроз	Уровень защищенности ПДн
1	1С: Предприятие	Клиент-сервер	2	ИНЫЕ	До 100000	Да / Да	3	4
2	АРМ «Директор»	Клиент-сервер	15	СПЕЦ	До 100000	Да/Да	3	3
3	Классный журнал	3-звенная	300	ИНЫЕ	До 100000	Да / Да	3	4

Также выделяют внешние подключения

Внешние ИС:

- АРМ ЕИОС КО
- Банк-онлайн
- Закупки
- Электронная отчетность

Требования к ним предъявляют владельцы ИС!

ТИПЫ ИС

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 N 149-ФЗ "ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ"

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

3) **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

5) **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

12) **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

Статья 6. Обладатель информации

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 13. Информационные системы

1. Информационные системы включают в себя:

1) государственные ИС - федеральные ИС и региональные ИС созданные на основании **федеральных законов**, **законов субъектов РФ**, **правовых актов** государственных органов;

2) муниципальные ИС, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

Государственные ИС

Ст.14.п1. ГИС создаются в целях реализации полномочий ОВ, обмена информацией между ОВ и в иных целях.

Ст.14.п9. Информация в ГИС является официальной.

Ст.13.п4. Требования ФЗ-149 для ГИС распространяются на Муниципальные ИС.

Защита ИСПДн, ГИС, МИС

Нормативные документы по защите ИСПДн (список)

- **Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) "О персональных данных"**
- **Постановление Правительства РФ** от 01.11.2012 **N 1119** "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных«
- **Приказ ФСТЭК России** от 18.02.2013 **N 21** "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн»
- **Приказ ФСБ России** от 10.07.2014 г. **N 378** "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
- **Приказ ФАПСИ** от 13.06.2001 **N 152 «**Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
- **Постановление Правительства Кировской области № 421 от 24.08.2017**

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 N 152-ФЗ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"

Статья 19. **Меры по обеспечению безопасности персональных данных при их обработке**

1. Оператор при обработке персональных данных **обязан принимать необходимые правовые, организационные и технические меры** или **обеспечивать их принятие** для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Статья 19. **Меры по обеспечению безопасности персональных данных при их обработке**

2. Обеспечение безопасности персональных данных достигается, в частности:

1) **определением угроз безопасности ПДн** при их обработке в ИСПДн;

2) применением **организационных и технических мер** по обеспечению безопасности ПДн при их обработке в ИСПДн, **необходимых** для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) **применением прошедших** в установленном порядке **процедуру оценки соответствия средств защиты информации**;

4) **оценкой эффективности принимаемых мер** по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

Статья 19. **Меры по обеспечению безопасности персональных данных при их обработке**

5) **учетом** машинных носителей ПДн;

6) **обнаружением** фактов несанкционированного доступа к ПДн и принятием мер;

7) **восстановлением** ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) **установлением правил доступа** к ПДн, обрабатываемым в ИСПДн, а также **обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн**;

9) **контролем за принимаемыми мерами** по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

Статья 19. **Меры по обеспечению безопасности персональных данных при их обработке**

3. Правительство РФ с учетом возможного вреда субъекту ПДн, **объема и содержания обрабатываемых персональных данных**, вида деятельности, при осуществлении которого обрабатываются персональные данные, **актуальности угроз безопасности** персональных данных устанавливает:

1) Уровни защищенности ПДн
2) Требования к защите ПДн
3) Требования к материальным носителям биометрических ПДн

Статья 19. **Меры по обеспечению безопасности персональных данных при их обработке**

4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите ПДн для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

Это:

- ФСБ России
- ФСТЭК России

Статья 19. **Меры по обеспечению безопасности персональных данных при их обработке**

5. Федеральные ОИВ, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, ОГВ субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют **угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных**, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 01.11.2012 N 1119

"ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ"

Постановление Правительства РФ от 01.11.2012 N 1119

- Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью системы защиты ПДн
- ЗС ПДн включает в себя: организационные и технические меры, определенные с учетом угроз безопасности ПДн
- Безопасность ПДн обеспечивает:
  - оператор ИСПДн
  - Лицо, которому поручено обрабатывать ПДн
- Выбор средств защиты выполняется по требованиям ФСБ и ФСТЭК

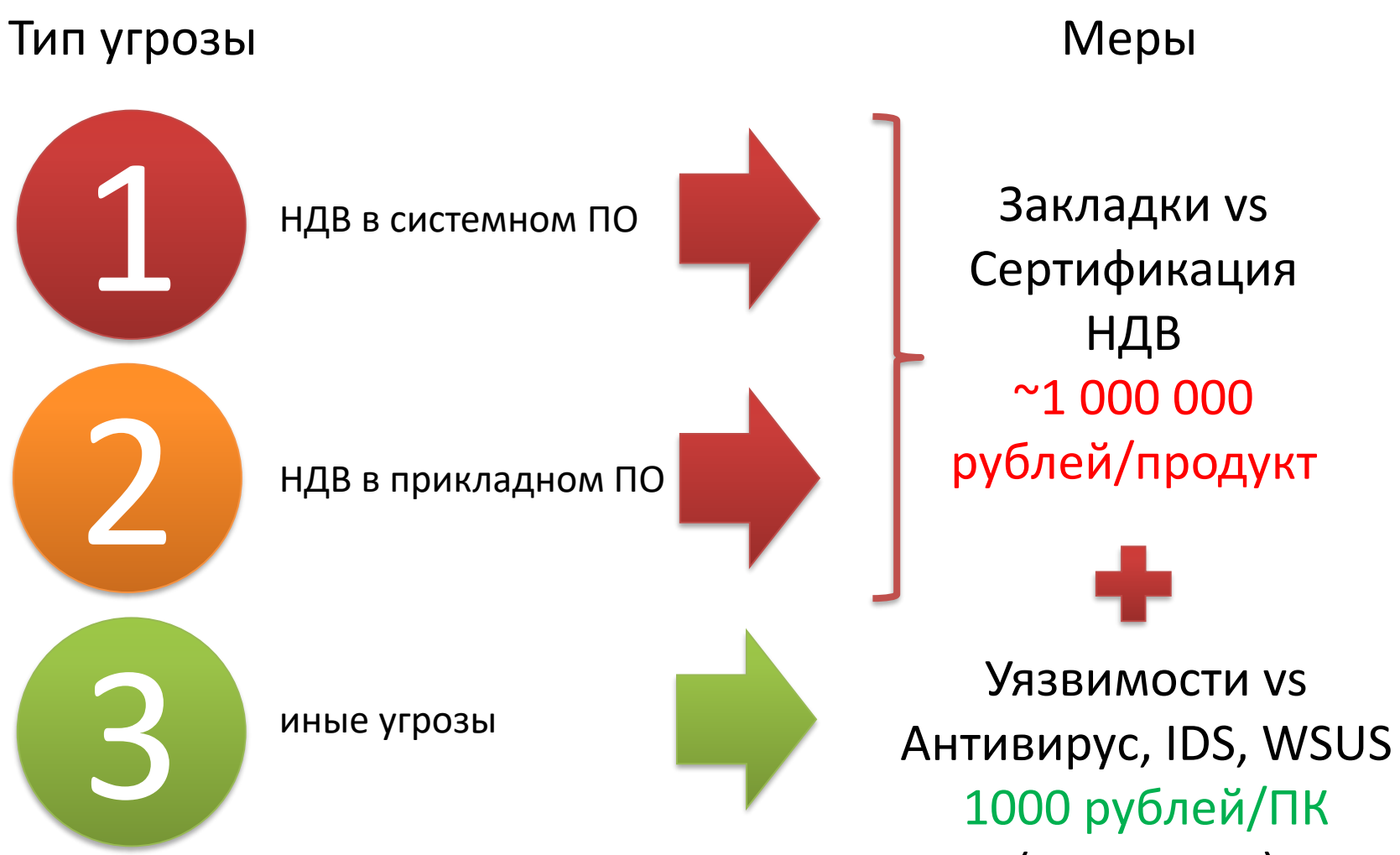
5. Типы ИСПДн

Тип	Категории персональных данных
ИСПДн-С	специальные (о расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни)
ИСПДн-Б	биометрические
ИСПДн-О	общедоступные
ИСПДн-И	иные

По принадлежности субъектов:

- **ИСПДн**, обрабатывающая **ПДн сотрудников** оператора.
- **ИСПДн**, обрабатывающая **ПДн субъектов** ПДн, **не являющихся сотрудниками** оператора**.**

6. Актуальные типы угроз



НДВ – недекларированные возможности (закладки)

Уровни защищенности ПДн

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-С	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 1	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 2	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4

99%

Меры согласно ПП 1119

Требования	Уровни защищенности			
	1	2	3	4
Режим обеспечения безопасности помещений, где обрабатываются персональные данных	+	+	+	+
Сохранность носителей персональных данные	+	+	+	+
Перечень лиц, допущенных к персональным данным	+	+	+	+
СЗИ, прошедшие процедуру оценки соответствия	+	+	+	+
Должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн	+	+	+	-
Ограничение доступа к содержанию электронного журнала сообщений	+	+	-	-
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным	+	-	-	-
Структурное подразделение, ответственное за обеспечение безопасности персональных данных	+	-	-	-

Контроль за выполнением ПП 1119

- 17. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности **по технической защите конфиденциальной информации**. Указанный контроль проводится **не реже 1 раза в 3 года** в сроки, определяемые оператором (уполномоченным лицом).

Три документа

- Акт классификации ИСПДн

  или

- Приказ о перечне ИСПДн

- Инструкция ответственного за ИБ

ПРИКАЗ ФСТЭК ОТ 18.02.2013 N 21

"ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ"

Приказ ФСТЭК от 18.02.2013 N 21

1. Устанавливает состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн

2. БПДн обеспечивают:

- оператор ИСПДн
- лицо, которому поручено обрабатывать ПДн
- для работ по БПДн могут по договору привлекаться лицензиаты ФСТЭК.

Приказ ФСТЭК от 18.02.2013 N 21

3. Меры должны быть направлены на нейтрализацию актуальных угроз безопасности ПДн.

4. Меры по обеспечению безопасности ПДн реализуются в том числе посредством применения в информационной системе **средств защиты информации**, **прошедших в установленном порядке процедуру оценки соответствия**, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

Приказ ФСТЭК от 18.02.2013 N 21

6. Оценка эффективности реализованных в рамках СЗ ПДН мер по обеспечению безопасности ПДн **проводится оператором самостоятельно** или с привлечением на договорной основе лицензиатов ФСТЭК.

Указанная оценка проводится не реже одного раза в 3 года.

Приказ 21 ФСТЭК

8. В состав мер по обеспечению безопасности ПДн входят:

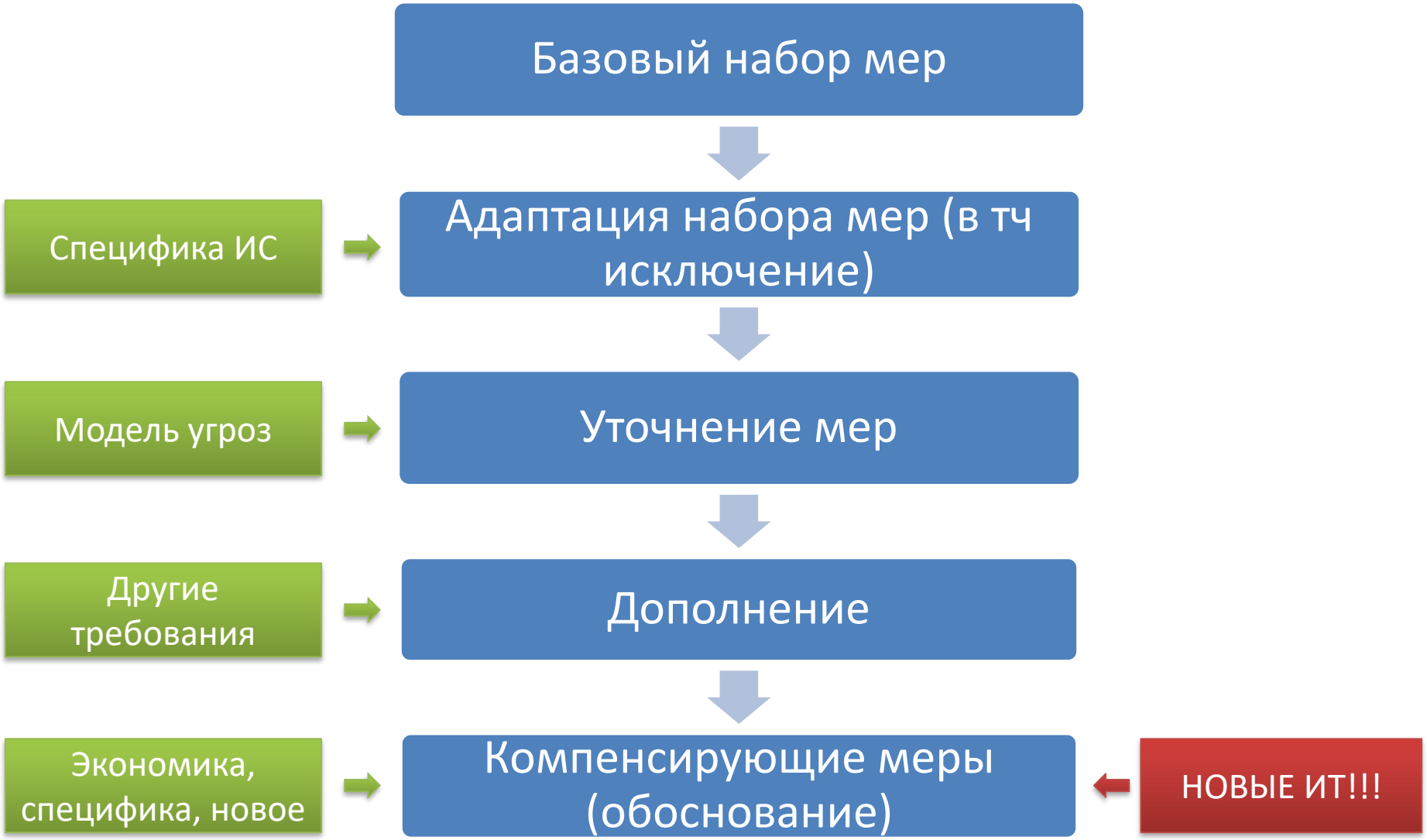
- идентификация и аутентификация (6);
- управление доступом (17);
- ограничение программной среды (4);
- защита машинных носителей информации (8);
- регистрация событий безопасности (8);
- антивирусная защита (2);
- обнаружение (предотвращение) вторжений (2);
- контроль (анализ) защищенности (5);
- обеспечение целостности (8);
- обеспечение доступности (7);
- защита среды виртуализации (10);
- защита технических средств (5);
- защита информационной системы, ее средств, систем связи (20);
- выявление инцидентов (6) – только в приказе № 21;
- управление конфигурацией ИС (4) – только в приказе № 21.

Меры по уровням защищенности:

- Всего мер - 112
- Базовых мер для УЗ 4 - 27
- Базовых мер для УЗ 3 - 41
- Базовых мер для УЗ 2 - 63
- Базовых мер для УЗ 1 - 69
- Всего дополнительных мер – 40

Но!!! В течение 2018 года данный перечень изменится для приведение в соответствие с 187-ФЗ «О безопасности критической информационной инфраструктуры»

Приказ ФСТЭК 21, 17
Процедура выбора мер



Сертифицированные СЗИ

12. Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

Уровень защищенности ПДн	Класс СЗИ, не ниже (МЭ, САВЗ, СОВ, СКН, СДЗ)	Класс РД, не ниже (СВТ)	Класс НДВ, не ниже
1	4	5	4
2	5	5	4
3	6	5	4 (при АУ2)
4	6	6	-

Ввод в эксплуатацию

ИСПДн:

- Оценка эффективности
- Оценка соответствия
- По акту о вводе в эксплуатацию

Государственные ИС:

- Аттестация
- П.17.3 – разрешена аттестация типовых сегментов

ПРИКАЗ ФСБ РОССИИ ОТ 10.07.2014 Г. N 378

"ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН ПРИ ИХ ОБРАБОТКЕ В ИСПДН С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, НЕОБХОДИМЫХ ДЛЯ ВЫПОЛНЕНИЯ УСТАНОВЛЕННЫХ ПРАВИТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ КАЖДОГО ИЗ УРОВНЕЙ ЗАЩИЩЕННОСТИ»

Приказ ФСБ России от 10.07.2014 г. N 378

- определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн (ИС) с использованием средств криптографической защиты информации (далее - СКЗИ)
- предназначен для операторов, использующих СКЗИ для обеспечения безопасности ПДн при их обработке в ИС

Приказ ФСБ России от 10.07.2014 г. N 378

- определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн (ИС) с использованием средств криптографической защиты информации (далее - СКЗИ)
- предназначен для операторов, использующих СКЗИ для обеспечения безопасности ПДн при их обработке в ИС

Приказ ФСБ России от 10.07.2014 г. N 378

- 4. Эксплуатация СКЗИ должна осуществляться **в соответствии с документацией на СКЗИ** и требованиями, установленными в настоящем документе, а также в соответствии с иными нормативными правовыми актами, регулирующими отношения в соответствующей области.

Требования П378

Оснащение помещений:

- замки;
- опечатывание или средства сигнализации;
- правила доступа в помещения (приказ о режиме);
- перечень допущенных лиц.

Требования П378

Машинные носители информации:

- хранение съемных МНИ в сейфах (опечатывание замочных скважин или кодовый замок);
- поэкземплярный учет МНИ.

Требования П378

Перечень пользователей ИСПДн:

- Утвердить;
- Поддерживать в актуальном состоянии.

Средства защиты:

- определить возможности нарушителя;
- использовать СКЗИ определенного класса.

Класс СКЗИ

Выбирается исходя из:

- возможностей нарушителя (след. семинар)
- Уровня защищенности ПДн

Классы СКЗИ в зависимости от уровня защищенности ПДн

4 уровень	3 уровень		2 уровень			1 уровень	
	2 типа	3 типа	1 типа	2 типа	3 типа	1 типа	2 типа
КС1	КВ1 КВ2 КА1	КС1 КС2 КС3 КВ1 КВ2 КА1	КА1	КВ1 КВ2 КА1	КС1 КС2 КС3 КВ1 КВ2 КА1	КА1	КВ1 КВ2 КА1
КС2							
КС3							
КВ1							
КВ2							
КА1							

КОНФИДЕНЦИАЛЬНЫЙ ДОКУМЕНТООБОРОТ

Конфиденциальный документооборот

Грифы ограничения доступа:

- Для служебного пользования (ДСП, ПП РФ №1233)
- Конфиденциально (Указ Президента №188 и законодательство РФ)
- Коммерческая тайна (закон №98-ФЗ)

Персональные данные:

- не грифуются
- организуются согласно ПП 687
- могут иметь гриф (см. вышеПП 687!!!).

Что относится к ДСП

ДСП - документы на основании решения руководителя органа федеральной власти

- антитеррористическая защищенность
- методические документы и некоторая переписка ФСТЭК
- документы об аттестации ИС
- некоторые виды переписок с федеральными органами власти

Что относится к КонфИ

Конфиденциальная информация, не составляющая государственную тайну:

- документы по защите информации
- документы по криптографии
- документы внутреннего пользования ограниченного доступа, не отнесенные к ДСП

КД - меры

- Гриф ограничения доступа

«Для служебного пользования

Экз №1»

- Поэкземплярный учет в журнале
- Учет ознакомления, выдачи, отправки, передачи

- Выделенное делопроизводство
  - Инструкция по КД
  - Номенклатура дел
  - Акты выделения к уничтожению
  - Акты уничтожения

КД – АРМ ЕИОС КО (2018)!!!

- Порядок - в инструкции по эксплуатации
- Ответственное лицо
- Хранение в одной папке
- Хранение в сейфе
- Опись документов
- Инвентаризация 1 раз в год

Ваши вопросы?

Спасибо за внимание!

Городилов Сергей

Руководитель направления ИБ, АСПЕКТ СПб

gors@aspectspb.ru

www.aspectspb.ru